Claims

What is claimed as being new and desired to be protected by Letters Patent of the United States as follows:

1. A method for operating a digital information processing system that encrypts information from a plurality of remote processors to a host processor or vice versa the method comprising processor executed steps of:

at the host and the remote processors before the start of encryption procedure:

means for assigning and mutually agreeing upon, a pre-determined number of bits that are located at pre-determined and specific positions, called Group and Function Bits, within a seed binary bit segment consisting of any length;

means for defining a plurality of function pool containing any type of mathematical or logical functions of any complexity;

means for establishing a unique relationship between the functions defined in the first pool with the functions defined in the second pool sequentially identical at both the host and the remote processors;

means for defining a number 'N' which indicates the total number of rounds used for encryption/decryption process.

at the remote processor:

(a) means for generating and sending a seed arbitrary binary bit segment consisted of any length to the host processor;

(b) means for processing the seed arbitrary binary bit segment at the remote processor;

(c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment;

(d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (b);

(e) means for identifying the corresponding single or plurality of mathematical or logical functions from the second pool;

(g) means for encrypting the digital information segment through operating single or plurality of mathematical or logical functions selected from the second function pool as described in step d;

(f) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step c;

(h) means for replacing the seed arbitrary binary bit segment with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment; and

(i) means for repeating the steps (b) to (h) 'N' times and then transmitting the resulting encrypted digital information segment to the said host.

2. The method and system according to claim 1 wherein the said method comprising processor executed steps of:

at the host processor:

(a) means for receiving and identifying the seed arbitrary binary bit segment from the said remote processor;

(b) means for processing the seed arbitrary binary bit segment;

(c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment;

(d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (c);

(e) means for identifying the corresponding single or plurality of mathematical or logical functions from the second pool;

(f) means for identifying the corresponding inverse function for each of the mathematical or logical functions as recognized in step (e) and tabulating the identified inverse mathematical or logical functions entries;

(g) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step d;

(h) means for replacing the seed arbitrary binary bit segment with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment; and

(i) means for repeating the steps (b) to (h) 'N' times and appending the inverse function entries resulting from each round into a tabular form.

3. The method and system according to claim 1 wherein the said method for operating a digital information processing system that decrypts information from a plurality of remote processors to a host processor or vice versa, the method comprising processor executed steps of:

at the host processor:

(a) means for receiving the encrypted digital information segment from the said remote processor;

(b) means for decrypting the digital information segment with the last inverse mathematical function entry as found in the table built in step (i) of claim 2;

(c) means for repeating the above step (b) until all the inverse mathematical or logical functions are exhausted as found in the built in table containing the inverse function entries.

4. The method and system according to claim 1 wherein the arbitrary binary bit segment can be a random number consisted of any arbitrary length.

5. The method and system according to claim 1 further comprising;

means for encrypting a seed binary bit segment through operating mathematical or logical functions which can result in a large bit size number; and

means for truncating the resulting large bit size number and reducing it to a pre-negotiated size mutually agreed between the said host and the remote.

6. The method and system according to claim 1 further comprising;

means for re-using the encrypted seed binary bit segment resulting from the previous encrypted round as a new seed binary bit segment for the next encryption rounds; and

means for encrypting the next digital information segments based on the information contained in the new seed binary bit segment.

7. The method and system according to claim 1 wherein the Group or Function Bits can mutually share the same single or plurality of bits located at pre-determined bit positions within a seed binary bit segment of any length.

8. The method and system according to claim 1 wherein any change in the Group or the Function Bits within a seed binary bit segment of any length leads to the selection of same or different set of mathematical or logical functions belonging to the first and second function pools.

9. The method and system according to claim 3 wherein the decryption procedure at the host processor comprises the steps of:

means for identifying the exact same Group or Function Bits as identified by the remote processor through the use of seed arbitrary binary bit segment;

means for identifying the exact same mathematical or logical functions from the first and the second function pools as identified by the remote processor; and

means for identifying single or plurality of inverse mathematical or logical functions corresponding to each of the identified function from the second pool to be utilized for decryption procedure.

10. The method and system according to claim 1 wherein the Group and the Function Bits located within a seed binary bit segment of any length can be uniquely assigned and mutually recognized through the use of any mathematical or logical functions of any complexity.

11. The method and system according to claim 7 further comprising:

means for reassigning and modifying the total number of Group and Function Bits within a seed binary bit segment in relation to the length range of the seed binary bit segment; and

means for selecting and using the same or a different set of mathematical or logical functions based upon the length range of a seed binary bit segment.

12. The method and system according to claim 1 wherein the transmitted encrypted digital information may consist of different number of bits than the original digital information segment.

13. The method and system according to claim 12 wherein the transmitted encrypted digital information segment further comprising:

means for containing a padding header followed by variable number of padding bit fields;

and means for making the total encrypted digital information segment bits exactly divisible by a specific number.

14. The method and system according to claim 1 wherein the remote and host processors mutually adopt and agree upon the use of a set of protocols and instructions to exchange configuration parameters and system information comprising:

means for reserving a specific bit at a pre-determined position in an information field such that the said bit value determines if the said information field is extended or span to include another known number of bits in the said field definition;

means for exchanging and modifying the total number of Group and Function Bits and their corresponding bit positions assigned within a seed binary bit segment consisting of any arbitrary length;

means for exchanging and modifying the unique association between Group or Function Bits numeric values and the corresponding mathematical or logical function;

means for exchanging a seed binary bit segment or a random number consisting of any arbitrary length through the use of an instruction format being processed as a part of system information; and means for using or designing any type of protocols or instructions formats to exchange any type of system or configuration information.

15. The method and system according to claim 14 wherein the remote exchanges the system or configuration information with the host processor or vice versa comprising;

means for receiving a public key from the host processor;

means for encrypting any type of system or configuration information through using the public key of the host processor;

means for transmitting the encrypted information to the host processor; and

means for decrypting the said received information at the host through using the host's private key.

16. The method and system according to claim 13 wherein the mutually adopted and agreed upon set of protocols uses a reserved single bit field appended at a pre-determined position known both to a host and a remote comprising,

means for assigning the first outcome of the said bit value to indicate user's information, and

means for assigning the second outcome of the said bit value to indicate system information.

17. The method and system according to claim 1 wherein the remote and host processors mutually agree on a procedure to verify the accuracy of encryption and decryption procedures, comprising:

means for calculating and appending a unique digital signature field reflecting the information contents of a digital information segment before the start of the encryption procedure at the remote processor;

means for calculating and verifying the same unique digital signature after decrypting the received digital information segment at the host processor; and

means for initializing different set of procedures if the verification process fails.

18. A method and system according to claim 1 wherein the remote and host processors mutually agree on a procedure to verify that the encrypted digital information is being delivered to an authenticated processor and the encryption/decryption procedures are working properly, comprising:

means for calculating and retaining a unique digital signature reflecting the information contents of a digital information segment before the start of the encryption procedure at the remote processor;

means for calculating the same unique digital signature after decrypting the received digital information segment at the host processor; and

means for encrypting and transmitting the said digital signature back to the originating remote processor;

means for comparing and verifying the received digital signature with the retained digital signature at the remote processor; and

means for initializing different set of procedures if the said verification process fails.

19. The method and system according to claim 1 wherein the type of digital information segment contains password information further comprising:

means for using any information contained within a random number to identify and determine specific bit locations in an arbitrary binary bit segment; and means for mapping single or plurality of bits belonging to the password information segment into the said specific bit locations of the arbitrary binary bit segment.

20. The method and system according to claim 1 wherein the type of digital information segment contains authentication information further comprising:

means for using any information contained within a password information segment to determine and identify specific bit locations in an arbitrary binary bit segment; and

means for mapping single or plurality of bits belonging to a random number segment into the said specific bit locations of the arbitrary binary bit segment.

21. A method for operating a digital information processing system that encrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of:

at the transmitting device:

means for generating a seed random number consisting of any arbitrary length and transmitting the said random number to the receiving device;

means for using the information contained in the random number to identify single or plurality of unique mathematical or logical functions identical at the both transmitting and the receiving devices;

means for encrypting any type of digital information consisted of any arbitrary length segment through operating the mathematical or logical functions;

means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round;

means for identifying the number of encryption rounds, N, through the use of any information means mutually agreed between the transmitting and the receiving devices; and

means for repeating the encryption process on the said digital information segment and the said random number for N number of rounds.

22. A method for operating a digital information processing system that decrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of:

at the receiving device:

means for receiving and identifying the seed random number of an arbitrary length from the transmitting device;

means for identifying the number of encryption rounds, N, through any means mutually agreed between the transmitting and the receiving devices;

means for using the information contained within the specific bits of the seed random number to identify a single or plurality of unique mathematical or logical functions;

means for identifying single or plurality of inverse functions corresponding to each of the identified mathematical or logical functions;

means for decrypting the received digital information segment through operating single or plurality of inverse functions;

means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round; and means for repeating the decryption process on the received digital information segment for N number of rounds to remove any effects of encryption on the said digital information segment.